David. S. Casey, Jr., SBN 060768
dcasey@cglaw.com
Gayle M. Blatt, SBN 122048
gmb@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811
Fax: (619) 544-9232

Attorneys for Plaintiffs and
the Putative Classes
[Additional Counsel Listed on Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL GREENSTEIN, CYNTHIA NELSON, AND SINKWAN AU on behalf of themselves and all other persons similarly situated,

Plaintiffs,

v.

NOBLR RECIPROCAL EXCHANGE, a Delaware corporation,

Defendant.

Case No. 4:21-cv-04537-JSW

FIRST AMENDED CLASS ACTION COMPLAINT

Demand for Jury Trial

Plaintiffs Michael Greenstein, Cynthia Nelson, and Sinkwan Au individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this First Amended Class Action Complaint against Defendant Noblr Reciprocal Exchange and allege as follows:

INTRODUCTION

1. Every year millions of Americans have their most valuable personal information stolen and sold online because of unauthorized data disclosures. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data about their customers or potential customers.

2. Defendant Noblr Reciprocal Exchange ("Defendant" or "Noblr"), provides insurance products, including car insurance, to Americans across the country. In doing so, it promises "[y]ou trust us with your information and we are committed to keeping that trust," "the security of your personal information is extremely important to us" and further promises in bold lettering "[w]e do not share your data or information without your permission."[1]

3. Noblr failed to meet these promises and its obligation to protect the sensitive personal information entrusted to it.

4. As reported by Noblr, on or about January 21, 2021, it "noticed unusual quote activity consisting of a spike in unfinished quotes through its instant quote webpage." It launched an investigation and learned that "attackers may have initiated these quotes in order to steal driver's license numbers which were inadvertently included in the page source code."[2] This means that for an unknown period of time before and including January 21, 2021, the drivers' license information of Plaintiffs and members of the class was publicly available via the page source code on Noblr's public website and being stolen by hackers.

---

[1] https://www.noblr.com/privacy-policy/

[2] https://media.dojmt.gov/wp-content/uploads/noblr-notif.pdf (last visited May 29, 2021).

5. As a corporation doing business in California, Noblr is legally required to protect the personal information ("PI") it gathers from unauthorized access and exfiltration.

6. As a result of Noblr's failure to provide reasonable and adequate data security, Plaintiffs' and the Class Members' PI has been exposed to those who should not have access to it. Plaintiffs and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after private PI stolen here.

THE PARTIES

7. Defendant Noblr Reciprocal Exchange is an unincorporated association domiciled in Colorado with its principal place of business in San Francisco, California. Noblr is an insurance provider currently providing insurance in Arizona, Colorado, Ohio, Louisiana, Maryland, Pennsylvania, New Mexico, and Texas, and has insurance licenses in all fifty states.

8. Plaintiff Michael Greenstein is a resident of Watchung, New Jersey. On or about May 2021, Plaintiff Greenstein received notice from Noblr that it improperly exposed his PI to unauthorized third parties. Plaintiff Greenstein never sought a quote for insurance of any sort from Defendant.

9. Plaintiff Cynthia Nelson is a resident of Watertown, Massachusetts. On or about May 2021, Plaintiff Nelson received notice from Noblr that it improperly exposed her PI to unauthorized third parties. Plaintiff never sought a quote for insurance of any sort from Defendant.

10. Plaintiff Sinkwan Au is a resident of Roslyn Heights, New York. On or about May 2021, Plaintiff Au received notice from Noblr that it improperly exposed her PI to unauthorized third parties. Plaintiff never sought a quote for insurance of any sort from Defendant.

JURISDICTION AND VENUE

11. Subject matter jurisdiction in this civil action is authorized pursuant to 28

U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims and supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in California, and has sufficient minimum contacts with California.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and on information and belief, a substantial part of the events or omissions giving rise to Plaintiffs' and Class Members' claims occurred in this District.

14. Application of California law to this dispute is proper because Defendant's headquarters are in California, the decisions, actions, and/or circumstances that gave rise to the underlying facts at issue in this Complaint were presumably made or taken in California, and the action and/or inaction at issue emanated from California.

INTRADISTRICT ASSIGNMENT

15. Pursuant to Civil L.R. 3-1 (c) and (d), assignment to the San Francisco Division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this district and specifically San Francisco County where Defendant is headquartered.

FACTUAL ALLEGATIONS

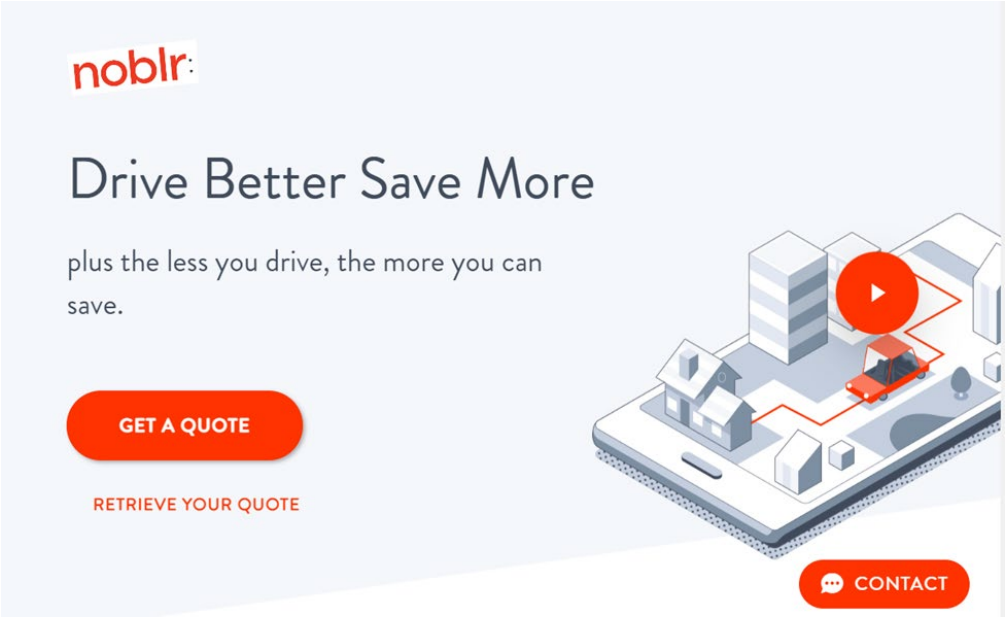
A. Noblr collects PI and fails to provide adequate data security

16. Noblr began as a car insurance start-up utilizing technology to provide a product to attract good drivers, "Using behaviour based pricing, Noblr calculated

insurance premiums in real-time based on how a driver performs."[3]

17. Noblr currently offers various types of insurance policies, including auto, renters, home and condo, and umbrella.[4]

18. Like other insurance providers, Noblr offers a public-facing insurance quoting platform for visitors on its website. Visitors to Noblr's website can "Get A Quote" instantly after providing personal information.



19. Noblr's quoting feature uses the information entered by the website's visitor, combines it with additional information the system matches, and then automatically pulls information from a third-party to provide the visitor a quote.

20. Unfortunately, Noblr's online quote system was configured to allow anyone with a few basic bits of data to get Noblr's system to auto-fill the remaining information, including driver's license numbers, from its databases, thus allowing hackers to steal that information.

21. On or around January 21, 2021, Noblr finally realized that its instant quote feature was being exploited by hackers who were using it to obtain the driver's

---

[3] https://www.artemis.bm/news/hudson-structured-invests-in-auto-insurtech-noblr/ (last visited May 29, 2021).

[4] https://www.noblr.com/coverages/

license numbers and addresses of Plaintiffs and the members of the Class, which includes many people who never applied for insurance with Noblr or were even aware of its existence.

22. This incident is referred to herein as the "Unauthorized Data Disclosure."

23. The named Plaintiffs received a letter from Noblr entitled "Notice of Data Security Incident Involving Your Personal Data," dated May 14, 2021. The letter stated that their PI, detailed below, may have been compromised, and included the following:

> **What Happened**
>
> On January 21, 2021, Noblr's web team noticed unusual quote activity consisting of a spike in unfinished quotes through its instant quote web page. Noblr immediately launched an internal investigation. The initial investigation revealed that attackers may have initiated these quotes in order to steal driver's license numbers which were inadvertently included in the page source code.
>
> As described above, the instant quote process works by taking personal data (name and date of birth) entered into the system and matching it with related information automatically pulled from a third-party to help provide a quote. The attackers appear to have already been in possession of the names and dates of birth of consumers, and then used that information to obtain additional personal information through Noblr's instant quote platform. Attackers could also have gone through the entire quote process to access personal information in the final policy application documents provided after obtaining a quote.
>
> On January 25, 2021, following the initial discovery of unusual quote activity, Noblr's security team began blocking suspicious IP addresses. On January 27, 2021, when Noblr determined that the attackers were able to access driver's license numbers, Noblr altered its instant quote system to prevent further access by the attackers and took other steps to combat these attacks.
>
> **What Information Was Involved**

> Our records indicate that your name, driver's license number, and address may have been accessed.
>
> **Actions We've Taken to Safeguard Your Information**
>
> We take our responsibility to safeguard your personal information seriously. We immediately took steps to remedy the situation, including blocking suspicious IP addresses, revising rate limit thresholds to adjust specific traffic patterns, and altering the instant quote system to mask driver's license numbers in the source code and in the final application page. In addition, we are developing and employing certain changes to processes and protocols to prevent this type of event from happening again.[5]

24. The Notice confirms that Plaintiffs became victims of the Unauthorized Data Disclosure even though they did not have a prior relationship with Noblr, advising "you may be affected even if you have no relationship with Noblr if your information, or the information of someone in your household, was used by the attackers in connection with this incident."

25. After receiving Unauthorized Data Disclosure notice letters, it is reasonable for Plaintiffs and Class Members in this case to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, in Noblr's letter it encourages affected individuals to use the identity theft protection service it offers to Plaintiffs and the Class to help protect their "identity from misuse" and that they should, among other things, "regularly review statements from your accounts and periodically obtain your credit report."

---

[5] Noblr's *Notice of Data Security Incident Involving Your Personal Information*, as filed with the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/c43bf2a1-cea9-45fa-81bf-47d299a7216d.shtml (last visited on May 29, 2021).

B. The PI exposed by Noblr as a result of its inadequate data security is highly valuable on the black market

26. The information exposed by Noblr is very valuable to phishers, hackers, identity thieves and cyber criminals, especially at this time where unprecedented numbers of fraudsters are filing fraudulent unemployment benefit claims.

27. Cybercrime has been on the rise for the past decade and continues to climb exponentially; as of 2013 it was being reported that nearly one out of four data breach notification recipients become a victim of identity fraud.[6]

28. Stolen PI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

29. When malicious actors infiltrate companies and copy and exfiltrate the PI that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[7]

30. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PI] belonging to victims from countries all over the world. One of the key challenges of protecting PI online is its pervasiveness. As unauthorized data disclosures in the news continue to show, PI about employees, customers and the

---

[6] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[7] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May. 29, 2021).

public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[8]

31. The PI of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[9]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[10].

32. The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Unauthorized Data Disclosure is difficult and likely highly problematic, to change— driver's licenses and addresses.

33. Recently, Forbes writer Lee Mathews reported on Geico's similar unauthorized data disclosure wherein the hackers also targeted driver's license numbers, "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license

---

[8] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 10, 2021).

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 29, 2021).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 29, 2021).

can sell for around $200."[11]

34. National credit reporting company, Experian, blogger Sue Poremba also emphasized the value of driver's license to thieves and cautioned:

> If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves.[12]

35. In fact, according to CPO Magazine, which specializes in news, insights and resources for data protection, privacy and cyber security professionals, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as

---

[11] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), *available at*: https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited May 29, 2021).

[12] Sue Poremba, *What should I do If My Driver's License Number is Stolen?* (Oct. 24, 2018), *available at*: https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited May 29, 2021).

unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."

36. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, indicating both that this particular form of PI is in high demand and also that Noblr knew or had reason to know that its security practices were of particular importance to safeguard consumer data.[13]

37. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

38. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

39. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and Class Members that their PI had been stolen. It took Noblr almost four months to do so.

---

[13] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (accessed Apr. 27, 2021) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021) (describing a scam involving drivers' license numbers and Progressive Insurance).

40. Victims of drivers' license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

41. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

42. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[14] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[15]

C. Noblr was on notice of the sensitivity and private nature of the PI it utilized for insurance quotes and its duty to safeguard it

43. "Insurance companies are desirable targets for cyber attackers because they work with sensitive data."[16] In fact, according to the Verizon 2020 Data Breach Investigations Report there were 448 confirmed data breaches in the financial and

---

[14] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited May 29, 2021).

[15] *Id.*

[16] Data Protection Compliance for the Insurance Industry (October 7, 2020), *available at*: https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry (last visited May 29, 2021).

insurance industries.[17]

44. Noblr claims it "uses commercially reasonable and industry standard administrative, technical, personnel, and physical security measures designed to protect the information we collect about you from loss, theft, and unauthorized use, disclosure, or modification," however, those safety and security measures were insufficient. And while Noblr states that the information is protected in an encrypted environment[18], it was not. The weakness in Noblr's system allowed access and ability to exfiltrate Plaintiffs' and the Class Members' addresses and driver's license numbers.

D. Noblr failed to comply with Federal Trade Commission requirements

45. Federal and State governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[19]

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[20] Among other things, the guidelines note businesses should properly dispose of personal information that is no

---

[17] Verizon 2020 Data Breach Investigations Report (2020), available at: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf (last visited May 29, 2021).

[18] *Id.*

[19] *See* Federal Trade Commission, *Start With Security* (June 2015), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 29, 2021).

[20] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 29, 2021).

longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

47. Also, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

48. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[23]

49. Through negligence in securing Plaintiffs' and Class Members' PI and allowing the thieves to utilize its instant quote website platform to obtain access and exfiltrate individuals' PI, Noblr failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class

---

[21] *Id.*

[22] Federal Trade Commission, *Start With Security*, *supra* footnote 25.

[23] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 8, 2021).

Members' PI. Noblr's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

E. Plaintiffs' attempts to secure their PI after the breach

Plaintiff Greenstein

50. In May 2021, Plaintiff Greenstein received notice from Noblr dated May 14, 2021("Notice Letter"). The Notice Letter informed him of the Unauthorized Data Disclosure and that his driver's license number and address may have been accessed.

51. Plaintiff Greenstein researched his options to respond to the theft of his driver's license. He spent and continues to spend additional time reviewing his credit monitoring service results and reports from other online resources concerning the security of his identity and financial information. This is time Plaintiff Greenstein otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

52. Plaintiff Greenstein has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

53. Plaintiff Greenstein suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) damages to and diminution in the value of his PI—a form of intangible property; (b) loss of his privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

54. As a result of the Unauthorized Data Disclosure, Plaintiff Greenstein will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Nelson

55. In May 2021, Plaintiff Nelson received notice from Noblr dated May 14, 2021 ("Notice Letter"). The Notice Letter informed her of the Unauthorized Data Disclosure and that her driver's license number and address may have been accessed.

56. As a result, Plaintiff Nelson notified her bank and financial planner of the Unauthorized Data Disclosure. She also contacted her local police department.

57. Plaintiff Nelson researched her options to respond to the theft of her driver's license. She spent and continues to spend additional time reviewing her credit monitoring service results and reports from other online resources concerning the security of her identity and financial information. This is time Plaintiff Nelson otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

58. Plaintiff Nelson has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. She deletes any and all electronic documents containing her PI and destroys any documents that contain any of her PI, or that may contain any information that could otherwise be used to compromise her PI.

59. Plaintiff Nelson suffered actual injury from having her PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) damages to and diminution in the value of her PI—a form of intangible property; (b) loss of her privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

60. As a result of the Unauthorized Data Disclosure, Plaintiff Nelson will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Au

61. In May 2021, Plaintiff Au received notice from Noblr dated May 14, 2021 ("Notice Letter"). The Notice Letter informed her of the Unauthorized Data

Disclosure and that her driver's license number and address may have been accessed. Her husband received a Notice Letter as well as to his own information.

62. Following the Unauthorized Data Disclosure, in January 2021, Plaintiff Au's data was fraudulently used to apply for unemployment benefits in New York.

63. As a result, Plaintiff Au contacted the local police department and filed a police report. She also filed a fraud report with New York State Department of Labor.

64. Plaintiff Au researched her options to respond to the theft of her driver's license identification and information, and took action including purchasing IDShield family plan credit monitoring for her and her husband for which she pays a monthly fee. She spent and continues to spend additional time reviewing her credit monitoring service results and reports from other online resources concerning the security of her identity and financial information. This is time Plaintiff Au otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

65. Plaintiff Au has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. She deletes any and all electronic documents containing her PI and destroys any documents that contain any of her PI, or that may contain any information that could otherwise be used to compromise her PI.

66. Plaintiff Au suffered actual injury from having her PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) damages to and diminution in the value of her PI—a form of intangible property; (b) loss of her privacy; and (c) fraud and imminent and impending injury arising from the increased risk of further fraud and identity theft.

67. As a result of the Unauthorized Data Disclosure, Plaintiff Au will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

F. Plaintiffs and Class Members suffered damages

68. Each of the Plaintiffs and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

69. The ramifications of Noblr's failure to keep individuals' PI secure are long lasting and severe. Once PI is stolen, fraudulent use of that information and damage to victims may continue for years.[24]

70. The PI belonging to Plaintiffs and Class Members is private, valuable and is sensitive in nature as it can be used to commit a lot of different harms in the hands of the wrong people. Defendant Noblr failed to obtain Plaintiffs' and Class Members' consent to disclose such PI to any other person as required by applicable law and industry standards.

71. Noblr's inattention to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's PI who utilized its front-facing instant quote platform left Plaintiff and Class Members with no ability to protect their sensitive and private information.

72. Noblr had the resources necessary to prevent the Unauthorized Data Disclosure, but neglected to adequately implement data security measures, despite its obligations to protect PI of the Plaintiffs and Class Members from unauthorized disclosure.

73. Had Noblr remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of PI.

74. As a direct and proximate result of Noblr's actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to

---

[24] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), *available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited May 29, 2021).

take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Unauthorized Data Disclosure on their lives.

75. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[25]

76. As a result of Noblr's failures to prevent the Unauthorized Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PI, which remains in the possession of Noblr and is subject to further breaches so long as Noblr fails to undertake appropriate measures to protect the PI in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of

[25] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited May 29, 2021).

the Unauthorized Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

77. In addition to a remedy for the economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further misappropriation and theft.

78. To date, other than providing 12 months of credit monitoring and identity protection services, Noblr does not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do the following:

- "regularly review statements from your accounts"
- "periodically obtain your credit report"
- "remain vigilant with respect to viewing your account statements and credit reports"
- obtain a copy of a free credit report
- contact the FTC and/or the state Attorney General's office to obtain additional information about avoiding identity theft

None of these recommendations, however, require Noblr to expend any effort to protect Plaintiffs' and Class Members' PI. It is also not clear that Noblr has made any determination that the credit monitoring and identity protection services are designed or adequate to ameliorate the specific harms of having an exposed driver's license number and address.

79. Noblr's failure to adequately protect Plaintiffs' and Class Members' PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Noblr's Notice indicates, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

80. Noblr's offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm

has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PI is acquired and when it is used.

G. **Noblr's delay in identifying and reporting the breach caused additional harm**

81. The actual date Plaintiffs and the Class Members' PI was improperly exposed is unknown to Plaintiffs at this time, however, Noblr discovered the Unauthorized Data Disclosure on or about January 21, 2021, and it was not until almost four months later that Noblr began notifying those affected by the Unauthorized Data Disclosure, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Unauthorized Data Disclosure.

82. As a result of Noblr's delay in detecting and notifying Plaintiffs and Class Members of the Unauthorized Data Disclosure, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

CHOICE OF LAW

83. Defendant Noblr is headquartered in San Francisco County, California. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

84. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's California headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Unauthorized Data Disclosure were made from and in California. Finally, Defendant's breach of its duty—including to Plaintiffs and Class and Subclass Members—emanated from California.

85. It is appropriate to apply California law extraterritorially to the claims against Defendant in this case due to Defendant's significant contacts with

California. Defendant is headquartered in California; the relevant decisions, actions, and omissions were made in California; and Defendant cannot claim to be surprised by application of California law to regulate its conduct emanating from California.

86. To the extent California law conflicts with the law of any other state that could apply to Plaintiffs' claims against Defendant, application of California law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

CLASS ACTION ALLEGATIONS

87. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class (the "Class"), defined as follows:

> All persons in the United States whose PI was compromised in the Unauthorized Data Disclosure announced by Noblr on or near May 14, 2021.

88. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Noblr; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

89. **Numerosity.** Members of the proposed Class likely number in at least the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

90. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein,

b. Whether Defendant's inadequate data security measures were a cause of the Unauthorized Data Disclosure,

c. Whether Defendant owed a legal duty to Plaintiffs and the other Class

Members to exercise due care in collecting, storing, and safeguarding their PI,

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI,

e. Whether Defendant's online quote system auto-populated prospective quotes with PI obtained from the records of Defendant or third parties without the permission or consent of Plaintiffs and the Class,

f. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the data security breach,

g. Whether Defendant's conduct violated Cal. Bus. & Prof Code § 17200 *et seq*.,

h. Whether Defendant failed to provide timely notice of the Unauthorized Data Disclosure to Plaintiffs and Class Members in violation of California Civil Code § 1798.82,

i. Whether Defendant violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724,

j. Whether Plaintiffs and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

k. Whether Plaintiffs and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

91. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

92. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. All Class Members were subject to the Unauthorized Data Disclosure and

had their PI accessed by, used and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

93. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

94. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724

(On behalf of Plaintiffs and the Nationwide Class)

95. Plaintiffs incorporate the above allegations by reference.

96. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information

pertains." 18 U.S.C. § 2724.

97. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(a). Drivers' license numbers are motor vehicle records under the DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 943 (7th Cir. 2015).

98. Defendant obtains motor vehicle records from its customers.

99. Defendant also obtains motor vehicle records directly from state agencies or through resellers who sell such records.

100. During the time period up until and including at least January 27, 2021, PI, including drivers' license numbers, of Plaintiffs and Class Members, were publicly available on Noblr's instant quote webpage and Noblr knowingly both used and disclosed Plaintiffs' and members of the class's motor vehicle records for a purpose not permitted by the DPPA pursuant to 18 U.S.C. §§ 2724 and 2721(b).

101. Through the Unauthorized Data Disclosure, Defendant disclosed motor vehicle records for purposes not authorized by the DPPA.

102. Plaintiffs and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

SECOND CAUSE OF ACTION

Negligence

(On behalf of Plaintiffs and the Nationwide Class)

103. Plaintiffs incorporate the above allegations by reference.

104. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining and testing its data security systems to ensure that

Plaintiffs' and Class Members' PI in Defendant's possession, or that could be accessed by Defendant, was adequately secured and protected.

105. Defendant owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected PI it stored, maintained, and/or obtained.

106. Defendant owed a duty of care to Plaintiffs and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in having its systems auto-populate online quote requests with private PI and without the consent or authorization of the person whose PI was being provided.

107. Unbeknownst to Plaintiffs and Members of the Class, they were entrusting Defendant with their PI when Defendant obtained their PI from other businesses. Defendant had an obligation to safeguard their information and was in a position to protect against the harm suffered by Plaintiffs and Members of the Class as a result of the Unauthorized Data Disclosure.

108. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendant's misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Unauthorized Data Disclosure.

109. Defendant knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendant knew about – or should have been aware of - numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

110. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PI of Plaintiffs and Class Members.

111. Because Defendant knew that a breach of its systems would damage

thousands of individuals whose PI was inexplicably stored or was accessible, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PI contained and/or accessible therein.

112. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' PI.

113. In engaging in the negligent acts and omissions as alleged herein, which permitted thieves to access Noblr's systems that stored and/or had access to Plaintiffs and Class Members' PI, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce," and the GLB Act. This includes failing to have adequate data security measures and failing to protect Plaintiffs' and the Class Members' PI.

114. Plaintiffs and the Class Members are among the class of persons Section 5 of the FTC and the GLB Act were designed to protect, and the injuries suffered by Plaintiffs and the Class Members are the types of injury Section 5 of the FTC Act and the GLB were intended to prevent.

115. Neither Plaintiffs nor the other Class Members contributed to the Unauthorized Data Disclosure as described in this Complaint.

116. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic

losses; (vii) the continued risk to their PI, which remains in Defendant's possession (and/or Defendant has access to) and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

THIRD CAUSE OF ACTION

Violation of the California's Unfair Competition Law

Cal. Bus. & Prof. Code § 17200, *et seq*.

(Brought by Plaintiffs and the Nationwide Class)

117. Plaintiffs incorporate the above allegations by reference.

118. By reason of the conduct alleged herein, Defendant Noblr engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

119. Defendant stored and/or provided access to the PI of Plaintiffs and all Class Members in its computer systems.

120. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiffs' and all Class Members' PI secure and prevented the loss or misuse of that PI.

Unlawful Business Practices

121. Defendant violated the DPPA, Section 5(a) of the FTC Act, the GLB Act and California Civil Code § 1798.81.5(b) by failing to implement and maintain reasonable and appropriate security measures or follow industry standards for data security, and by failing to timely notify Plaintiffs and all Class Members of the Unauthorized Data Disclosure.

122. If Defendant had complied with these legal requirements, Plaintiffs and

the Class Members would not have suffered the damages related to the Unauthorized Data Disclosure, and Defendant's notification of it.

123. Plaintiffs and all Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiffs and all Class Members' PI was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and all Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

124. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, none of Defendant's actions or inactions can be said to have had any utility at all. Defendant's failures were clearly injurious to Plaintiffs and all Class Members, directly causing the harms alleged below.

125. Defendant also engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation

of the law.

126. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects tens of thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and all Class Members' PI to third parties without their consent, diminution in value of their PI, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and all Class Members' PI remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); see also, e.g., *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

127. Plaintiffs and all Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiffs and all Class Members' PI was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and all Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

128. As a result of Defendant's unlawful and unfair business practices in

violation of the UCL, Plaintiffs and all Class Members are entitled to equitable and injunctive relief, including restitution or disgorgement.

FORTH CAUSE OF ACTION

Declaratory and Injunctive Relief

(Brought by Plaintiffs and the Nationwide Class)

129. Plaintiffs incorporate the above allegations by reference.

130. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

131. As previously alleged, Plaintiffs and Class Members had a reasonable expectation that companies such as Defendant, who could access their PI through automated systems, would provide adequate security for that PI.

132. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PI.

133. Defendant still possesses PI regarding Plaintiffs and Class Members.

134. Since the Unauthorized Data Disclosure, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks.

135. The Unauthorized Data Disclosure has caused actual harm because of Defendant's failure to fulfill its duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendant's failure to address the security failings that lead to such exposure.

136. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Unauthorized Data Disclosure to meet Defendant's legal duties.

137. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its duties of care to provide adequate security,

and (2) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring,

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures,

d. Ordering that Defendant not transmit PI via unencrypted email and not be permitted to put PI as part of its source code or otherwise be available on its instant quote webpage,

e. Ordering that Defendant not store or make accessible PI in any publicly facing website,

f. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services,

g. Ordering that Defendant conduct regular computer system scanning and security checks, and

h. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request that the Court enter an order:

a. Certifying the proposed Class as requested herein,

b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class

Counsel,

c. Finding that Defendant engaged in the unlawful conduct as alleged herein,

d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Noblr from engaging in the wrongful and unlawful acts described herein,

ii. requiring Noblr to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

iii. requiring Noblr to delete, destroy, and purge the personal information of Plaintiffs and Class Members unless Noblr can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members,

iv. requiring Noblr to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiffs and Class Members' personal information,

v. prohibiting Noblr from maintaining Plaintiffs' and Class Members' personal information on a cloud-based database,

vi. requiring Noblr to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Noblr's systems on a periodic basis, and ordering Noblr to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring Noblr to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring Noblr to audit, test, and train its security personnel regarding any new or modified procedures,

ix. requiring Noblr to conduct regular database scanning and securing checks,

x. requiring Noblr to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiffs and Class Members,

xi. requiring Noblr to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring Noblr to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Noblr's policies, programs, and systems for protecting personal information,

xiii. requiring Noblr to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Noblr's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring Noblr to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

information to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring Noblr to design, maintain, and test its computer systems to ensure that PI in its possession is adequately secured and protected,

xvi. requiring Noblr disclose any future data disclosures in a timely and accurate manner; and

xvii. requiring Defendant to provide ongoing credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiffs and Class Members damages,

f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest on all amounts awarded,

g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: July 1, 2021

/s/ Gayle M. Blatt
GAYLE M. BLATT

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
David S. Casey, Jr.
dcasey@cglaw.com
Gayle M. Blatt
gmb@cglaw.com
P. Camille Guerra
camille@cglaw.com
110 Laurel Street
San Diego, CA 92101

Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Kate M. Baxter-Kauf (MN #0392037)
Karen Hanson Riebel (MN #0219770)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com